CODE LOOPS IN DIMENSION AT MOST 8

E.A. O'BRIEN AND PETR VOJTĚCHOVSKÝ

Abstract. Code loops are certain Moufang 2-loops constructed from doubly even binary codes that play an important role in the construction of local subgroups of sporadic groups. More precisely, code loops are central extensions of the group of order 2 by an elementary abelian 2-group V in the variety of loops such that their squaring map, commutator map and associator map are related by combinatorial polarization and the associator map is a trilinear alternating form.

Using existing classifications of trilinear alternating forms over the field of 2 elements, we enumerate code loops of dimension $d = \dim(V) \leq 8$ (equivalently, of order $2^{d+1} \leq 512$) up to isomorphism. There are 767 code loops of order 128, and 80826 of order 256, and 937791557 of order 512.

1. Introduction

Code loops are certain Moufang 2-loops constructed from doubly even binary codes that play an important role in the construction of local subgroups of sporadic groups [1, 9, 19].

We enumerate the code loops of order 128, 256 and 512 up to isomorphism, so extending the work of Nagy and Vojtěchovský [26]. The results are summarized in Tables 1 and 2. The code loops can be constructed explicitly; those of orders dividing 256 will be available in a future release of the LOOPS package [27] for GAP [13].

The theoretical results required for the classification of code loops were described briefly in [26], in the context of a larger project of enumerating all Moufang loops of order 64. Since our work suggests that it will be difficult to extend the classification of code loops beyond order 512 (see Remark 4.1), we carefully record the theory here.

In Section 2 we recall the necessary background material on Moufang loops, code loops, symplectic 2-loops, trilinear alternating forms, combinatorial polarization and small Frattini Moufang loops. In particular, we recall that code loops, symplectic Moufang 2-loops and small Frattini Moufang 2-loops are the same objects. The group $GL(V)$ acts naturally on the set F^V of maps $V \to F$ by

$$f \mapsto f^S, \quad f^S(u) = f(uS^{-1}).$$

We show that two code loops, realised as central extensions of the two-element field $F = \mathbb{F}_2$ by a vector space V over F, are isomorphic if and only if their squaring maps $x \mapsto x^2$ (which can be realised as maps $V \to F$) lie in the same orbit of this action.

For $f \in F^V$ with $f(0) = 0$, the mth derived form f_m of f is the symmetric map $V^m \to F$ defined by

$$f_m(v_1, \ldots, v_m) = \sum_{\emptyset \neq I \subseteq \{1,\ldots,m\}} (-1)^{m-|I|} f(\sum_{i \in I} v_i). \tag{1.1}$$

2010 *Mathematics Subject Classification.* Primary: 20N05. Secondary: 15A69, 20B25, 20B40.

Key words and phrases. Code loop, doubly even code, trilinear alternating form, Moufang loop, general linear group, sporadic group, the Monster group.

O'Brien was supported by the Marsden Fund of New Zealand via grant UOA 1323. Vojtěchovský was supported by Simons Foundation Collaboration Grant 210176 and PROF Grant of the University of Denver.

If $P : V \to F$ is the squaring map of a code loop Q, then $P_2 = C : V^2 \to F$ is the commutator map of Q, $P_3 = A : V^3 \to F$ is the associator map of Q, and $P_4 = 0$. Let

$$F_4^V = \{f \in F^V \mid f(0) = 0,\ f_4 = 0\},$$

so that F_4^V consists of maps $f : V \to F$ such that f_3 is a trilinear alternating form. The results of Section 2 imply that $f \in F^V$ is the squaring map of a code loop if and only if $f \in F_4^V$.

In Section 3 we therefore study the action of $GL(V)$ on F^V restricted to F_4^V, whose orbits are in one-to-one correspondence with code loops of order $n = 2^{\dim(V)+1}$ up to isomorphism. Suppose that V has ordered basis $(e_1, \dots, e_d)$. A map $f \in F_4^V$ is uniquely determined by the values

$$\omega_{i_1 \cdots i_k} = f_k(e_{i_1}, \dots, e_{i_k}) \in F, \tag{1.2}$$

where $1 \le k \le 3$ and $1 \le i_1 < \cdots < i_k \le d$. Conversely, given arbitrary parameters $\omega_{i_1 \cdots i_k} \in F$ for every $1 \le k \le 3$ and $1 \le i_1 < \cdots < i_k \le d$, there is a unique map $f \in F_4^V$ such that (1.2) holds. The action of $GL(V)$ on F_4^V is therefore equivalent to a certain action of $GL(V)$ on the parameter space

$$\Omega_d = F^{\binom{d}{1}+\binom{d}{2}+\binom{d}{3}}.$$

The action of $GL(V)$ on Ω_d is stratified in a sense defined in Section 3.3, and its orbits can thus be calculated in three steps as in Corollary 3.8, the result on which our calculations are based.

The first step is a linear action of $G = GL(V)$ on $F^{\binom{d}{3}}$, which is equivalent to the classification of trilinear alternating forms over F in dimension d. It is not hard to calculate orbit representatives when $d \le 6$. For $d \ge 7$, we use the existing classifications of [7] ($d = 7$) and [21] ($d = 8$), where orbit representatives and the orders of their automorphism groups are given. We explicitly calculate the automorphism groups, so verifying these results. The trilinear alternating forms $A : V^3 \to F$ correspond to the associator maps in code loops. Given a trilinear alternating form A, the second step amounts to understanding the orbits and stabilizers of affine actions of the stabilizer G_A on $F^{\binom{d}{2}}$. The resulting symmetric alternating maps $C : V^2 \to F$ correspond to the commutator maps in code loops. Given a map C from the second step, the third step consists of calculating orbits of affine actions of the stabilizer $G_{A,C}$ on $F^{\binom{d}{1}}$. The resulting maps $P : V \to F$ correspond to the squaring maps in code loops.

Our results and information about the calculations are recorded in Section 4.

2. Preliminaries

2.1. **Loops and Moufang loops.** A nonempty set Q with a binary operation $\cdot$ and an element 1 is a *loop* if $x \cdot 1 = 1 \cdot x = x$ for every $x \in Q$ and if the translations $L_x : Q \to Q$, $L_x(y) = x \cdot y$ and $R_x : Q \to Q$, $R_x(y) = y \cdot x$ are bijections of Q for every $x \in Q$. We often write xy instead of $x \cdot y$.

A loop Q is *Moufang* if it satisfies the identity $x(y(xz)) = ((xy)x)z$. Moufang loops form a variety of loops with properties close to groups. For instance, any two elements of a Moufang loop generate a group, and if $x(yz) = (xy)z$ for some elements x, y, z of a Moufang loop, then the subloop generated by x, y, z is a group [24]. As a significant nonassociative example, nonzero octonions under multiplication form a Moufang loop.

For a prime p, a *p-loop* is a loop whose order is a power of p.

2.2. **Code loops.** Code loops were introduced in 1986 by Griess [19] as follows.

Let $F = \mathbb{F}_2$. Given $u = (u_1, \dots, u_d) \in F^d$, let $|u| = \sum_{i=1}^d u_i \in \mathbb{Z}$ be the Hamming weight of u. Given $u = (u_1, \dots, u_d)$ and $v = (v_1, \dots, v_d) \in F^d$, let $u \cap v = (u_1 v_1, \dots, u_d v_d)$, where $u_i v_i = 1$ if and only if $u_i = 1 = v_i$.

Let V be a doubly even binary code, that is, a linear subspace of F^d such that $|u| \equiv 0 \pmod 4$ for every $u \in V$. Note that then $|u|/4$, $|u \cap v|/2$ and $|u \cap v \cap w|$ are integers for every u, v, $w \in V$. A function $\theta : V^2 \to F$ is a *factor set* if

$$\begin{aligned}
&\theta(u,u) \equiv |u|/4 \pmod 2,\\
&\theta(u,v) + \theta(v,u) \equiv |u \cap v|/2 \pmod 2,\\
&\theta(u,v) + \theta(u+v,w) + \theta(v,w) + \theta(u,v+w) \equiv |u \cap v \cap w| \pmod 2,
\end{aligned}$$

for all u, v, $w \in V$.

A *code loop* Q is a loop defined on $F \times V$ by

$$(a,u)(b,v) = (a + b + \theta(u,v), u + v),$$

where V is a doubly even binary code and $\theta : V^2 \to F$ is a a factor set.

Griess [19] proved that every doubly even code admits a factor set, the isomorphism type of a code loop over V is independent of the choice of the factor set θ, and every code loop is Moufang. Furthermore, he showed that code loops correspond to a certain class of loops considered by Parker (see [19, Definition 13, Theorem 14]), which were in turn used by Conway as one of the key steps in the construction of the Monster sporadic group [9]. In the language of code loops, the Parker loop for the Monster group is the code loop associated with the extended binary Golay code.

2.3. **Symplectic 2-loops.** The connection between sporadic groups and Moufang 2-loops was reinforced by Aschbacher [1, Chapters 4 and 10]. To explain his results on loops, we first introduce central extensions of loops and symplectic 2-loops.

The *center* of a loop Q consists of all $x \in Q$ such that $xy = yx$, $x(yz) = (xy)z$, $y(xz) = (yx)z$ and $y(zx) = (yz)x$ for every y, $z \in Q$. The center $Z(Q)$ is a normal subloop of Q (that is, a kernel of a loop homomorphism).

A loop Q is a *central extension* of an abelian group $(Z,+)$ by a loop $(V,+)$ if $Z \le Z(Q)$ and Q/Z is isomorphic to V. Up to isomorphism, all central extensions of Z by V are obtained as loops $Q(Z,V,\theta)$ defined on $Z \times V$ with multiplication

$$(a,u)(b,v) = (a + b + \theta(u,v), u + v),$$

where $\theta : V^2 \to Z$ is a map satisfying $\theta(0,u) = \theta(u,0) = 0$ for every $u \in V$.

The *commutator* $C(x,y)$ of $x, y \in Q$ is the unique element of Q such that $xy = (yx)C(x,y)$, and the *associator* $A(x,y,z)$ of $x, y, z \in Q$ is the unique element of Q such that $(xy)z = (x(yz))A(x,y,z)$.

Following [1], a loop Q is a *symplectic 2-loop* if it is a central extension of the 2-element group $(Z,+) = (\mathbb{F}_2,+)$ by an elementary abelian 2-group $(V,+)$. Direct calculation shows that the squaring map $P : Q \to Q$, $x \mapsto x^2$, the commutator map $C : Q^2 \to Q$, $(x,y) \mapsto C(x,y)$, and the associator map $A : Q^3 \to Q$, $(x,y,z) \mapsto A(x,y,z)$ are given by

$$\begin{aligned}
P(a,u) &= (\theta(u,u), 0),\\
C((a,u),(b,v)) &= (\theta(u,v) + \theta(v,u), 0),\\
A((a,u),(b,v),(c,w)) &= (\theta(u,v) + \theta(u+v,w) + \theta(v,w) + \theta(u,v+w), 0).
\end{aligned}$$

All three maps are therefore well-defined modulo Z, and can be viewed as maps $P : V \to \mathbb{F}_2$, $C : V^2 \to \mathbb{F}_2$, $A : V^3 \to \mathbb{F}_2$.

Comparing this with Griess' definition of a factor set, we see that code loops are symplectic 2-loops over a doubly even binary code $(V,+)$ in which the squaring map, the commutator map and the associator map are governed by natural intersection properties of codewords of V.

2.4. **Trilinear alternating forms.** Let V be a vector space over a field F. A map $f : V^m \to F$ is *symmetric* if $f(v_1, \ldots, v_m) = f(v_{\pi(1)}, \ldots, v_{\pi(m)})$ for every $v_1, \ldots, v_m \in V$ and every $\pi \in S_m$; it is *m-linear* if it is linear in every coordinate; and it is *alternating* if $f(v_1, \ldots, v_m) = 0$ whenever $v_i = v_j$ for some $1 \le i < j \le m$. If F has characteristic 2, then it is easily seen that every m-linear alternating form is symmetric.

Two m-linear alternating forms f, $g : V^m \to F$ are *equivalent* if there is $S \in GL(V)$ such that $f(v_1, \ldots, v_m) = g(v_1S, \ldots, v_mS)$ for every $v_1, \ldots, v_m \in V$. Trilinear alternating forms over $\mathbb{F}_2$ have been classified up to equivalence in dimensions $d = \dim(V) \le 8$; see [7] for $d \le 7$ and [21] for $d = 8$.

Suppose $(e_1, \ldots, e_d)$ is an ordered basis of V. A trilinear alternating form $f : V^3 \to \mathbb{F}_2$ is determined by the values $f(e_{i_1}, e_{i_2}, e_{i_3})$ with $1 \le i_1 < i_2 < i_3 \le d$. As usual, we therefore represent alternating forms in a compact notation that indicates for which triples $(e_{i_1}, e_{i_2}, e_{i_3})$ the form does not vanish. For instance, $f = 123 + 145$ is the form $f : V^3 \to \mathbb{F}_2$ such that $f(e_{i_1}, e_{i_2}, e_{i_3}) = 1$ if and only if $\{i_1, i_2, i_3\} \in \{\{1, 2, 3\}, \{1, 4, 5\}\}$.

2.5. **Combinatorial polarization.** To identify Moufang loops among symplectic 2-loops, we need the notion of combinatorial polarization due to Ward [30]. We follow the terminology and notation of [1].

Let F be a field, V a vector space over F, and $f : V \to F$ a map satisfying $f(0) = 0$. For $m \ge 1$, the *mth derived form* of f is the map $f_m : V^m \to F$ defined by (1.1). Note that (1.1) is an analog of the principle of inclusion and exclusion for maps. For instance,

$$f_3(v_1, v_2, v_3) = f(v_1 + v_2 + v_3) - f(v_1 + v_2) - f(v_1 + v_3) - f(v_2 + v_3) + f(v_1) + f(v_2) + f(v_3).$$

Further note that $f_1 = f$ and every f_m is symmetric. The maps f_1, f_2, ... are *related by polarization*. It is not difficult to show that if f_1, f_2, ... are related by polarization, then

$$f_{m+1}(v_1, \ldots, v_{m+1}) = f_m(v_1 + v_2, v_3, \ldots, v_{m+1}) - f_m(v_1, v_3, \ldots, v_{m+1}) - f_m(v_2, v_3, \ldots, v_{m+1}) \tag{2.1}$$

for every $m \ge 1$ and $v_1, \ldots, v_{m+1} \in V$. Conversely, if $f_m : V^m \to F$ are symmetric maps satisfying (2.1) for every $m \ge 1$ and $v_1, \ldots, v_{m+1} \in V$, then f_1, f_2, ... are related by polarization.

We record additional consequences of (2.1) whenever f_1, f_2, ... are related by polarization:

- $f_{m+1} = 0$ if and only if f_m is additive in every coordinate,
- $f_m(v_1, \ldots, v_m) = 0$ whenever $v_i = 0$ for some i,
- if F has characteristic 2 then f_m is alternating.

Consequently, if $F = \mathbb{F}_2$ then $f_{m+1} = 0$ if and only if f_m is an m-linear alternating form.

2.6. **Symplectic Moufang 2-loops.** Let V be a vector space over $F = \mathbb{F}_2$. The group $GL(V)$ acts on the space of maps $f : V \to F$ by

$$f^S(v) = f(vS^{-1}),$$

where $S \in GL(V)$ and $v \in V$. This is indeed an action since $f^{ST}(v) = f(v(ST)^{-1}) = f(vT^{-1}S^{-1}) = f^S(vT^{-1}) = (f^S)^T(v)$. (See Section 3.4 for a discussion of related actions.)

Aschbacher [1, Lemma 13.1, Lemma 13.5, Theorem 13.7] proved the following.

- A symplectic 2-loop $Q = Q(F, V, \theta)$ is Moufang if and only if the maps P, C, A are related by polarization, that is, $C = P_2$ and $A = P_3$.
- Given a map $f : V \to F$ such that $f(0) = 0$, there is a symplectic Moufang 2-loop with $P = f$ if and only if $f_4 = 0$, or, equivalently, if and only if f_3 is a trilinear alternating form.
- Two symplectic Moufang 2-loops over V are isomorphic if and only if their squaring maps are in the same orbit of the action of $GL(V)$ on F_4^V.

2.7. **Small Frattini Moufang loops.** Hsu [22] showed that the code loops of Griess are precisely the symplectic Moufang 2-loops of Aschbacher.

Let p be a prime and let Q be a Moufang p-loop. Glauberman and Wright [16, 17] showed that Q is centrally nilpotent. Let $\Phi(Q)$ be the *Frattini subloop* of Q, consisting of all nongenerators of Q. Bruck [4] showed that $\Phi(Q)$ is the smallest normal subloop of Q such that $Q/\Phi(Q)$ is an elementary abelian p-group. Following [22], a Moufang p-loop Q is *small Frattini* if $|\Phi(Q)| \in \{1, p\}$, and an associative small Frattini Moufang p-loop is a *small Frattini group*. It was shown in [22] that $\Phi(Q) \le Z(Q)$ in every small Frattini Moufang p-loop Q. Hence the small Frattini Moufang 2-loops are precisely the symplectic Moufang 2-loops. Hsu [22] also proved the following.

- A nonassociative small Frattini Moufang p-loop exists if and only if $p \in \{2, 3\}$.
- Small Frattini Moufang 2-loops (hence symplectic Moufang 2-loops) are precisely the code loops.

2.8. **Related results.** Chein and Goodaire [6] used an intricate combinatorial construction to show that code loops are precisely Moufang loops with at most two squares. Their construction is used in [22] and generalized in [29].

If $f : V^3 \to \mathbb{F}_2$ is a trilinear alternating form, then its *radical* is $\{v_1 \in V \mid f(v_1, v_2, v_3) = 0$ for every v_2, $v_3 \in V\}$. The radical and *radical polynomial* are key invariants of trilinear alternating forms [21]. Drápal and Vojtěchovský [11] showed that if a Moufang loop Q has an associator map with trivial radical that is equivalent to an associator map of a code loop, then Q is also a code loop. Moreover, they proved that two code loops with equivalent associators can be obtained from one another by a sequence of two kinds of constructions, known as cyclic and dihedral modifications.

Hsu [23] presented an iterative construction that builds a code loop from a given doubly even binary code. Nagy [25] presented a global construction of code loops based on groups with triality associated with Moufang loops. His construction can be used to construct explicitly code loops from the parameters (1.2).

We do not pursue here the connections between code loops and sporadic groups [1, 9, 19]. In this direction, the notion of a code loop has been extended to odd primes in [20, 28]. An attempt to unify the theory of code loops for $p = 2$ and p odd has been made in [12].

3. The action of $GL(V)$

Combining the results of Aschbacher and Hsu, we obtain the following.

Theorem 3.1 ([1], [22])**.** *Let $d \ge 3$, $F = \mathbb{F}_2$, $V = F^d$, and let $F_4^V = \{f : V \to F \mid f(0) = 0$ and $f_4 = 0\}$. The code loops of order 2^{d+1} up to isomorphism are in one-to-one correspondence with orbits of the action of $GL(V)$ on F_4^V given by $f^S(u) = f(uS^{-1})$.*

In Section 3.1 we show that a map $f \in F_4^V$ can be described by $\binom{d}{1} + \binom{d}{2} + \binom{d}{3}$ parameters in F. In Section 3.2 we exhibit the action of $GL(V)$ on the parameter space $\Omega_d = F^{\binom{d}{1}+\binom{d}{2}+\binom{d}{3}}$ that is equivalent to the action of $GL(V)$ on F_4^V. In Section 3.3 we show how to iteratively calculate the orbits of $GL(V)$ on Ω_d by restricting the action to various subspaces of Ω_d.

3.1. **Combinatorial polarization with a fixed basis.** Let $F = \mathbb{F}_2$, and let V be a vector space over F with ordered basis $(e_1, \dots, e_d)$. For $u = \sum_{i=1}^d u_i e_i$ let

$$|u| = \sum_{i=1}^{d} u_i \in \mathbb{Z}.$$

Lemma 3.2. *Let V be a vector space over $F = \mathbb{F}_2$ with ordered basis $(e_1, \dots, e_d)$. If $f : V \to F$ satisfies $f(0) = 0$ and $f_{m+1} = 0$, then f is uniquely determined by the parameters* (1.2) *with $1 \le k \le m$ and $1 \le i_1 < i_2 < \cdots < i_k \le d$.*

Proof. We show by induction on $|u|$ that $f(u)$ is determined for every $u \in V$. If $|u| = 0$ then $u = 0$ and $f(0) = 0$ is given. Suppose that $|u| > 0$ and $f(v)$ is determined for every $v \in V$ with $|v| < |u|$. Then there exist $i_1 < \cdots < i_k$ such that $u = \sum_i u_i e_i = e_{i_1} + \cdots + e_{i_k}$. By (1.1),

$$f(u) = f_k(e_{i_1}, \ldots, e_{i_k}) + \sum_I f(\sum_{i \in I} u_i e_i) = \omega_{i_1 \cdots i_k} + \sum_I f(\sum_{i \in I} u_i e_i),$$

where the summation runs over all nonempty, proper subsets I of $\{i_1, \ldots, i_k\}$. By the induction assumption, $f(\sum_{i \in I} u_i e_i)$ is known for each such subset I. If $k > m$ then $\omega_{i_1 \cdots i_k} = 0$. Otherwise $k \leq m$ and $\omega_{i_1 \cdots i_k}$ is one of the given parameters. □

The following result is essentially [22, Theorem 8.3] combined with the remarks therein. It allows us to reconstruct explicitly the symmetric maps f, f_2 and f_3 from the parameters (1.2) whenever $f_4 = 0$.

Proposition 3.3. *Let V be a vector space over $F = \mathbb{F}_2$ with ordered basis $(e_1, \ldots, e_d)$. If $f : V \to F$ satisfies $f(0) = 0$ and $f_4 = 0$, then*

$$\begin{aligned} & f_3(\sum_i x_i e_i, \sum_j y_j e_j, \sum_k z_k e_k) \\ &= \sum_{i,j,k} x_i y_j z_k \omega_{ijk} \\ &= \sum_{i<j<k} (x_i y_j z_k + x_i y_k z_j + x_j y_i z_k + x_j y_k z_i + x_k y_i z_j + x_k y_j z_i) \omega_{ijk} \end{aligned} \tag{3.1}$$

for every x_i, y_j, $z_k \in F$,

$$\begin{aligned} & f_2(\sum_i x_i e_i, \sum_j y_j e_j) \\ &= \sum_{i,j} x_i y_j \omega_{ij} + \sum_k \sum_{i<j} x_i x_j y_k \omega_{ijk} + \sum_i \sum_{j<k} x_i y_j y_k \omega_{ijk} \\ &= \sum_{i<j} (x_i y_j + x_j y_i) \omega_{ij} + \sum_{i<j<k} (x_i x_j y_k + x_i x_k y_j + x_j x_k y_i + x_i y_j y_k + x_j y_i y_k + x_k y_i y_j) \omega_{ijk} \end{aligned} \tag{3.2}$$

for every x_i, $y_j \in F$, and

$$f(\sum_i x_i e_i) = \sum_i x_i \omega_i + \sum_{i<j} x_i x_j \omega_{ij} + \sum_{i<j<k} x_i x_j x_k \omega_{ijk} \tag{3.3}$$

for every $x_i \in F$.

Proof. In both (3.1) and (3.2) the second equality follows from the fact that each f_k is symmetric and alternating. We therefore prove only the first equality in each of (3.1), (3.2), (3.3).

Since $f_4 = 0$, the form f_3 is trilinear and (3.1) follows.

We prove (3.2) by induction on $|x| + |y|$. If $|x| \leq 1$ and $|y| \leq 1$, the result immediately follows because the sums with $i < j$ and $j < k$ are vacuous, and the first sum involves at most one summand. By symmetry, we can now assume without loss of generality that $|x| \geq 2$ and write

$x = x' + x''$, where $|x'| < |x|$ and $|x''| < |x|$. By (2.1), the inductive assumption and (3.1),

$$\begin{aligned}
f_2(\sum_i (x'_i + x''_i)e_i, \sum_j y_j e_j) \\
&= f_2(\sum_i x'_i e_i, \sum_j y_j e_j) + f_2(\sum_i x''_i e_i, \sum_j y_j e_j) + f_3(\sum_i x'_i e_i, \sum_j x''_j e_j, \sum_k y_k e_k) \\
&= \sum_{i,j} x'_i y_j \omega_{ij} + \sum_k \sum_{i<j} x'_i x'_j y_k \omega_{ijk} + \sum_i \sum_{j<k} x'_i y_j y_k \omega_{ijk} \\
&\quad + \sum_{i,j} x''_i y_j \omega_{ij} + \sum_k \sum_{i<j} x''_i x''_j y_k \omega_{ijk} + \sum_i \sum_{j<k} x''_i y_j y_k \omega_{ijk} \\
&\quad + \sum_{i,j,k} x'_i x''_j y_k \omega_{ijk}.
\end{aligned}$$

We need to show that this is equal to

$$\sum_{i,j} (x'_i + x''_i) y_j \omega_{ij} + \sum_k \sum_{i<j} (x'_i + x''_i)(x'_j + x''_j) y_k \omega_{ijk} + \sum_i \sum_{j<k} (x'_i + x''_i) y_j y_k \omega_{ijk}.$$

Clearly, the sums involving ω_{ij} agree, and so do the sums involving $y_j y_k$. Since

$$\sum_{i<j} (x'_i + x''_i)(x'_j + x''_j) = \sum_{i<j} x'_i x'_j + \sum_{i<j} x''_i x''_j + \sum_{i,j} x'_i x''_j,$$

the remaining sums also agree.

Finally, we prove (3.3) by induction on $|x|$. There is again nothing to show when $|x| \leq 1$, so suppose that $|x| \geq 2$ and let x', x'' be such that $x = x' + x''$, $|x'| < |x|$ and $|x''| < |x|$. By (2.1), the inductive assumption, (3.1) and (3.2),

$$\begin{aligned}
f(\sum_i (x'_i + x''_i)e_i) &= f(\sum_i x'_i e_i + \sum_i x''_i e_i) \\
&= f(\sum_i x'_i e_i) + f(\sum_i x''_i e_i) + f_2(\sum_i x'_i e_i, \sum_j x''_j e_j) \\
&= \sum_i x'_i \omega_i + \sum_{i<j} x'_i x'_j \omega_{ij} + \sum_{i<j<k} x'_i x'_j x'_k \omega_{ijk} \\
&\quad + \sum_i x''_i \omega_i + \sum_{i<j} x''_i x''_j \omega_{ij} + \sum_{i<j<k} x''_i x''_j x''_k \omega_{ijk} \\
&\quad + \sum_{i,j} x'_i x''_j \omega_{ij} + \sum_k \sum_{i<j} x'_i x'_j x''_k \omega_{ijk} + \sum_i \sum_{j<k} x'_i x''_j x''_k \omega_{ijk}.
\end{aligned}$$

We leave as an exercise for the reader to show that this is equal to

$$\sum_i (x'_i + x''_i)\omega_i + \sum_{i<j} (x'_i + x''_i)(x'_j + x''_j)\omega_{ij} + \sum_{i<j<k} (x'_i + x''_i)(x'_j + x''_j)(x'_k + x''_k)\omega_{ijk}. \qquad \square$$

We now show the converse of Lemma 3.2, namely that the parameters (1.2) determine a map $f \in F_4^V$.

Proposition 3.4. *Let V be a vector space over $F = \mathbb{F}_2$ with ordered basis $(e_1, \ldots, e_d)$. Suppose that the parameters $\omega_{i_1 \cdots i_k}$ of (1.2) are given for every $1 \leq k \leq 3$ and $1 \leq i_1 < \cdots < i_k \leq d$. Define $f_3 : V^3 \to F$, $f_2 : V^2 \to F$ and $f_1 = f : V \to F$ according to (3.1), (3.2) and (3.3), respectively. Then f_1, f_2, f_3 are related by polarization and $f_4 = 0$.*

Proof. The formulas (3.1), (3.2), (3.3) produce symmetric maps f_3, f_2, f_1, respectively. To show that f_1, f_2, f_3 are related by polarization, it therefore suffices to check that (2.1) holds. Let $x = \sum_i x_i e_i$, $y = \sum_j y_j e_j$ and $z = \sum_k z_k e_k$.

The left hand side of

$$f_3(x, y, z) = f_2(x + y, z) - f_2(x, z) - f_2(y, z)$$

is equal to

$$f_3(\sum_i x_i e_i, \sum_j y_j e_j, \sum_k y_k e_k) = \sum_{i,j,k} x_i y_j z_k \omega_{ijk},$$

while the right hand side is equal to

$$\begin{aligned}
&f_2(\sum_i (x_i + y_i)e_i, \sum_j z_j e_j) - f_2(\sum_i x_i e_i, \sum_j z_j e_j) - f_2(\sum_i y_i e_i, \sum_j z_j e_j) \\
&\quad = \sum_{i,j} (x_i + y_i) z_j \omega_{ij} + \sum_k \sum_{i<j} (x_i + y_i)(x_j + y_j) z_k \omega_{ijk} + \sum_i \sum_{j<k} (x_i + y_i) z_j z_k \omega_{ijk} \\
&\qquad - \sum_{i,j} x_i z_j \omega_{ij} - \sum_k \sum_{i<j} x_i x_j z_k \omega_{ijk} - \sum_i \sum_{j<k} x_i z_j z_k \omega_{ijk} \\
&\qquad - \sum_{i,j} y_i z_j \omega_{ij} - \sum_k \sum_{i<j} y_i y_j z_k \omega_{ijk} - \sum_i \sum_{j<k} y_i z_j z_k \omega_{ijk}.
\end{aligned}$$

In this expression, the summands involving ω_{ij} cancel, and so do all the summands involving $z_j z_k$. Therefore the right hand side reduces to

$$\sum_k \sum_{i<j} (x_i y_j + y_i x_j) z_k \omega_{ijk},$$

and equality follows.

Similarly, in

$$f_2(x, y) = f(x + y) - f(x) - f(y)$$

the left hand side is equal to

$$\sum_{i,j} x_i y_j \omega_{ij} + \sum_k \sum_{i<j} x_i x_j y_k \omega_{ijk} + \sum_i \sum_{j<k} x_i y_j y_k \omega_{ijk},$$

while the right hand side is equal to

$$\begin{aligned}
&f(\sum_i (x_i + y_i)e_i) - f(\sum_i x_i e_i) - f(\sum_i y_i e_i) \\
&\quad = \sum_i (x_i + y_i)\omega_i + \sum_{i<j} (x_i + y_i)(x_j + y_j)\omega_{ij} + \sum_{i<j<k} (x_i + y_i)(x_j + y_j)(x_k + y_k)\omega_{ijk} \\
&\qquad - \sum_i x_i \omega_i - \sum_{i<j} x_i x_j \omega_{ij} - \sum_{i<j<k} x_i x_j x_k \omega_{ijk} \\
&\qquad - \sum_i y_i \omega_i - \sum_{i<j} y_i y_j \omega_{ij} - \sum_{i<j<k} y_i y_j y_k \omega_{ijk}.
\end{aligned}$$

It can be seen easily that the two sides are equal.

Finally, since f_3 is trilinear and alternating, $f_4 = 0$. □

3.2. **The action of $GL(V)$ on the parameter space Ω_d.** By Propositions 3.3 and 3.4, we can identity the space F_4^V with the space of parameters

$$\omega_i,\, \omega_{ij},\, \omega_{ijk} \in F,$$

where $1 \le i < j < k \le d$. We write the parameter space as

$$\Omega_d = \bigoplus_I Fe_I,$$

where the summation runs over all subsets $I = \{1, \dots, d\}$ such that $1 \le |I| \le 3$. In particular, Ω_d has dimension $\binom{d}{1} + \binom{d}{2} + \binom{d}{3}$.

An element of Ω_d is written either as a sum $\sum_I \omega_I e_I$, or as a tuple $(\omega_I)_I$, where the subsets I are first ordered by cardinality and then lexicographically. For instance, an element of Ω_3 is

$$(\omega_1,\, \omega_2,\, \omega_3,\, \omega_{12},\, \omega_{13},\, \omega_{23},\, \omega_{123}).$$

We now describe the action of $GL(V)$ on Ω_d that is equivalent to the natural action of $GL(V)$ on F_4^V.

Proposition 3.5. *Let V be a vector space over $F = \mathbb{F}_2$ with ordered basis $(e_1, \dots, e_d)$. Let $S \in GL(V)$ and $T = (t_{ij}) = S^{-1}$. Let $\omega \in \Omega_d$. The coordinates of ω^S are obtained as follows:*

$$\omega^S_{uvw} = \sum_{i<j<k} (t_{ui}t_{vj}t_{wk} + t_{ui}t_{vk}t_{wj} + t_{uj}t_{vi}t_{wk} + t_{uj}t_{vk}t_{wi} + t_{uk}t_{vi}t_{wj} + t_{uk}t_{vj}t_{wi})\omega_{ijk}$$

for every $1 \le u < v < w \le d$,

$$\begin{aligned}\omega^S_{uv} =& \sum_{i<j} (t_{ui}t_{vj} + t_{uj}t_{vi})\omega_{ij} \\ &+ \sum_{i<j<k} (t_{ui}t_{uj}t_{vk} + t_{ui}t_{uk}t_{vj} + t_{uj}t_{uk}t_{vi} + t_{ui}t_{vj}t_{vk} + t_{uj}t_{vi}t_{vk} + t_{uk}t_{vi}t_{vj})\omega_{ijk}\end{aligned}$$

for every $1 \le u < v \le d$, and

$$\omega^S_u = \sum_i t_{ui}\omega_i + \sum_{i<j} t_{ui}t_{uj}\omega_{ij} + \sum_{i<j<k} t_{ui}t_{uj}t_{uk}\omega_{ijk}$$

for every $1 \le u \le d$.

Proof. Let $f \in F_4^V$ be the unique map such that (1.2) holds for every $1 \le i_1 < i_2 < i_3 \le d$. Let $1 \le u < v < w \le d$. Now (3.1) implies that

$$\omega^S_{uvw} = f_3^S(e_u, e_v, e_w) = f_3(e_uT, e_vT, e_wT) = f_3(\sum_i t_{ui}e_i, \sum_j t_{vj}e_j, \sum_k t_{wk}e_k)$$

is equal to

$$\sum_{i<j<k} (t_{ui}t_{vj}t_{wk} + t_{ui}t_{vk}t_{wj} + t_{uj}t_{vi}t_{wk} + t_{uj}t_{vk}t_{wi} + t_{uk}t_{vi}t_{wj} + t_{uk}t_{vj}t_{wi})\omega_{ijk},$$

as claimed. The other two formulas follow analogously from (3.2) and (3.3), respectively. □

To understand the action of $GL(V)$ on Ω_d, we decompose Ω_d as follows. For $1 \le k \le 3$, let

$$\Omega_d[k] = \sum_{|I|=k} Fe_I,$$

and for $\omega \in \Omega_d$ let $\omega[k]$ be the projection of ω onto $\Omega_d[k]$. Thus $\omega = \omega[1] \oplus \omega[2] \oplus \omega[3]$.

Proposition 3.6. *Let V be a vector space over $F = \mathbb{F}_2$ with ordered basis $(e_1, \dots, e_d)$, and let $S \in GL(V)$. For every $\omega \in \Omega_d$, there are square matrices*

$$N_1 \in M_{\binom{d}{1}}(F), \quad N_2 \in M_{\binom{d}{2}}(F), \quad N_3 \in M_{\binom{d}{3}}(F)$$

(which depend on S but are independent of ω) and vectors

$$\nu_1(\omega[2], \omega[3]) \in F^{\binom{d}{1}}, \quad \nu_2(\omega[3]) \in F^{\binom{d}{2}}$$

(which depend on S and the components of ω as indicated) such that

$$\omega^S = (\omega[1] \oplus \omega[2] \oplus \omega[3])^S = (\omega[1]N_1 + \nu_1(\omega[2], \omega[3])) \oplus (\omega[2]N_2 + \nu_2(\omega[3])) \oplus (\omega[3]N_3).$$

Proof. This follows immediately from Proposition 3.5. For instance, with $T = (t_{ij}) = S^{-1}$, the entry in row ij and column uv of N_2 is $t_{ui}t_{vj} + t_{uj}t_{vi}$, and the entry in column uv of $\nu_2(\omega[3])$ is

$$\sum_{i<j<k} (t_{ui}t_{uj}t_{vk} + t_{ui}t_{uk}t_{vj} + t_{uj}t_{uk}t_{vi} + t_{ui}t_{vj}t_{vk} + t_{uj}t_{vi}t_{vk} + t_{uk}t_{vi}t_{vj})\omega_{ijk}. \qquad \square$$

In particular, the following hold.

- The restriction of the action of $G = GL(V)$ onto $\Omega_d[3]$ induces a linear action on $\Omega_d[3]$, namely $\omega[3]^S = \omega[3]N_3$.
- For $A \in \Omega_d[3]$, let G_A be the stabilizer of A under the above action of G on $\Omega_d[3]$. Then G_A induces an affine action on $\Omega_d[2] \oplus A$, namely $(\omega[2] \oplus A)^S = (\omega[2]N_2 + \nu_2(A)) \oplus A$.
- For $A \in \Omega_d[3]$ and $C \in \Omega_d[2]$, let $G_{C \oplus A}$ be the stabilizer of C under the above action of G_A on $\Omega_d[2] \oplus A$. Then $G_{C \oplus A}$ induces an affine action on $\Omega_d[1] \oplus C \oplus A$, namely $(\omega[1] \oplus C \oplus A)^S = (\omega[1]N_1 + \nu_1(C, A)) \oplus C \oplus A$.

3.3. **Stratified group actions.** For a group G acting on a set X, let X/G denote the set of all orbit representatives of G on X. We now describe the orbit representatives of actions that behave analogously to the action of $GL(V)$ on Ω_d.

Let $X = X_1 \times \cdots \times X_m$ be a set and suppose that a group G acts on X. The action of G on X is *stratified* (with respect to the decomposition $X_1 \times \cdots \times X_m$) if:

(i) for every $1 \le i \le m$ the action of G on X induces an action on $X_i \times \cdots \times X_m$, and
(ii) for every $1 < i \le m$ and every $(x_i, \dots, x_m) \in X_i \times \cdots \times X_m$ the stabilizer $G_{(x_i, \dots, x_m)}$ induces an action on $X_{i-1} \times (x_i, \dots, x_m)$.

Proposition 3.7. *If the action of a group G on $X = X_1 \times \cdots \times X_m$ is stratified, then X/G consists of all tuples $(x_1, \dots, x_m)$, where*

$$x_m \in X_m/G, \quad x_{m-1} \in (X_{m-1} \times x_m)/G_{x_m}, \quad \dots \quad , \quad x_1 \in (X_1 \times (x_2, \dots, x_m))/G_{(x_2, \dots, x_m)}.$$

Proof. We prove the claim by induction on m. If $m = 1$, we need to show that $X/G = X_1/G$, which is certainly true.

Suppose that $m = 2$ and let $(y_1, y_2) \in X_1 \times X_2$. There is a unique $x_2 \in X_2/G$ such that $y_2^G = x_2^G$. Let $g \in G$ and $z_1 \in X_1$ be such that $(y_1, y_2)^g = (z_1, x_2)$. There is a unique $x_1 \in X_1/G_{x_2}$ such that $(z_1, x_2)^{G_{x_2}} = (x_1, x_2)^{G_{x_2}}$.

Finally, suppose that $m > 2$ and the claim is true for $m - 1$. With $X_2' = X_2 \times \cdots \times X_m$, we see that the action of G is also stratified with respect to the decomposition $X_1 \times X_2'$. The result follows from the case $m = 2$ and the inductive assumption. $\square$

By Proposition 3.6, the action of $GL(V)$ on the parameter space Ω_d is stratified with respect to the decomposition $\Omega_d[1] \oplus \Omega_d[2] \oplus \Omega_d[3]$. We deduce the following from Proposition 3.7 and Theorem 3.1.

Corollary 3.8. *Let $d \geq 3$ and let V be a vector space over $\mathbb{F}_2$ with ordered basis $(e_1, \ldots, e_d)$. Then $G = GL(V)$ acts on the parameter space Ω_d as in Proposition 3.5, and the orbits of G are in one-to-one correspondence with code loops of order 2^{d+1} up to isomorphism. Moreover, Ω_d/G consists of all vectors $w[1] \oplus w[2] \oplus w[3]$ such that*

$$w[3] \in \Omega_d[3]/G, \quad w[2] \in (\Omega_d[2] \oplus w[3])/G_{w[3]}, \quad w[1] \in (\Omega_d[1] \oplus w[2] \oplus w[3])/G_{w[2] \oplus w[3]}.$$

3.4. **Related actions.** Our enumeration is based on the usual action of $GL(V)$ on F^V, namely $\varphi(S)(f) = f^S$, $f^S(v) = f(vS^{-1})$. The reason for the inverse in the formula is best seen by considering a copy W of V. If S is a bijection $V \to W$ and $f \in F^V$, then $f^S \in F^W$ and we demand $f(v) = f^S(vS)$ for all $v \in V$, or, equivalently, $f^S(w) = f(wS^{-1})$ for all $w \in W$. By contrast, the enumeration of [26] was based on the action $\psi(S)(f)(v) = f(vS^t)$, where S^t is the transpose of S. We show that both actions yield the same orbits on Ω_d and hence the same code loops up to isomorphism.

Lemma 3.9. *Let G be a group and α an involutory automorphism of G. Let φ be an action of G on a set X, and let ψ be the action of G on X defined by $\psi(g) = \varphi(g^\alpha)$. If $H \leq G$ and $x \in X$, then $\mathrm{Stab}(H, x, \varphi)^\alpha = \mathrm{Stab}(H^\alpha, x, \psi)$ and $\mathrm{Orb}(H, x, \varphi) = \mathrm{Orb}(H^\alpha, x, \psi)$.*

Proof. If $g \in \mathrm{Stab}(H, x, \varphi)$ then $g^\alpha \in H^\alpha$ and $\psi(g^\alpha)(x) = \varphi(g)(x) = x$, so $g^\alpha \in \mathrm{Stab}(H^\alpha, x, \psi)$. Conversely, if $g^\alpha \in \mathrm{Stab}(H^\alpha, x, \psi)$ then $g \in H$ and $\varphi(g)(x) = \psi(g^\alpha)(x) = x$, so $g^\alpha \in \mathrm{Stab}(H, x, \varphi)^\alpha$. Thus $y = \varphi(g)(x)$ for some $g \in H$ if and only if $y = \psi(g^\alpha)(x)$ for some $g^\alpha \in H^\alpha$. □

Consider now the involutory automorphism α of $GL(V)$ given by $S^\alpha = S^{-t}$. Observe that $\varphi(S^\alpha)(f)(v) = f(v(S^{-1})^{-t}) = f(vS^t) = \psi(S)(f)(v)$. Similar observations hold for the actions of $GL(V)$ on multivariate maps, which we also denote by φ and ψ. Lemma 3.9 therefore applies, and we use it repeatedly.

If $A \in \Omega_d[3]$, then $H = \mathrm{Stab}(G, A, \varphi) = \mathrm{Stab}(G, A, \psi)^\alpha$ and $\mathrm{Orb}(G, A, \varphi) = \mathrm{Orb}(G, A, \psi)$. If $C \in \Omega_d[2]$, then $K = \mathrm{Stab}(H, C, \varphi) = \mathrm{Stab}(H^\alpha, C, \psi)^\alpha$ and $\mathrm{Orb}(H, C, \varphi) = \mathrm{Orb}(H^\alpha, C, \psi)$. Finally, if $P \in \Omega_d[1]$, then $\mathrm{Stab}(K, P, \varphi) = \mathrm{Stab}(K^\alpha, P, \psi)^\alpha$ and $\mathrm{Orb}(K, P, \varphi) = \mathrm{Orb}(K^\alpha, P, \psi)$.

4. The results

d	0	1	2	3	4	5	6	7	8
n	2	4	8	16	32	64	128	256	512
ℓ_n	1	2	4	10	23	88	767	80826	937791557
s_n	1	2	4	5	7	8	10	11	13
m_n	1	2	5	19	122	4529	?	?	?
g_n	1	2	5	14	51	267	2328	56092	10494213

Table 1. Enumeration of certain classes of Moufang loops of order $n = 2^{d+1}$ up to isomorphism

4.1. **Code loops of given order.** Table 1 summarizes the results obtained by an algorithm based on Corollary 3.8. For $n = 2^{d+1}$ with $0 \leq d \leq 8$, Table 1 gives the number ℓ_n of code loops of order n up to isomorphism and the number s_n of small Frattini groups of order n up to isomorphism. For comparison, we give the number m_n of Moufang loops of order n up to isomorphism and the number g_n of groups of order n up to isomorphism.

Only the numbers ℓ_{128}, ℓ_{256}, ℓ_{512} are new. The numbers g_n and s_n are recorded in [14]. (We can also obtain s_n by applying our algorithm to vectors $\omega = \omega[1] \oplus \omega[2] \oplus \omega[3]$ with $\omega[3] = 0$, that is, with trivial associator map.) It is known that all Moufang loops of order less than 12 are associative [5]. For m_{16} and m_{32}, see [5, 18]. We obtain ℓ_{16} and ℓ_{32} from [18] or `LOOPS`. For m_{64} and ℓ_{64}, see [26] or `LOOPS`.

4.2. **Code loops with a prescribed associator.** We now give more detailed computational results and also summarise the techniques used in our computations. Most of the computations were carried out using GAP Version 4.7.9 on a computer with a 2.9 GHz processor.

For $n \leq 128$, Corollary 3.8 can be routinely turned into an efficient algorithm. The running time for $n \leq 64$ is in seconds, and for $n = 128$ in minutes. For $n \geq 256$, the computational difficulties are considerable and additional improvements must be employed. We discuss the most difficult case where $n = 512$ and $d = 8$, the case 256 is similar.

There are 12 trilinear alternating forms in dimension 7 [7], and 32 in dimension 8 [21]. Hora and Pudlák [21] used radical polynomials and other invariants to construct 32 inequivalent forms in dimension 8, and then employed the Orbit-Stabilizer Theorem to check that their list of forms is complete.

We used the trilinear alternating forms of [21] and independently verified their stabilizer claims. For each trilinear alternating form A in dimension 8, we used randomized techniques, similar to those described in [15, §8], to construct a subgroup H_A of the stabilizer G_A of A under the action of $G = GL(8, \mathbb{F}_2)$. We used the explicit matrix action of G in dimension $\binom{8}{3} = 56$ as given in Proposition 3.5. If G_A is small, then this technique sometimes produced only a proper subgroup H_A of G_A; if so, we constructed the stabilizer of the form explicitly in $N_G(H_A)$, so obtaining a larger H_A. Finally, we verified that $\sum_A [G : H_A] = 2^{56}$, which implies that $H_A = G_A$ for all A. This calculation was carried out using MAGMA [3] and took about 7 days of CPU time.

For each A and G_A, we then calculated the orbits of the action of G_A on the $\binom{8}{2} = 28$-dimensional vector space $\Omega_8[2]$ (more precisely, on the coset $\Omega_8[2] \oplus A$), by converting the affine action of Proposition 3.5 into a permutation action. It took about 2 hours per generator to construct the permutations for G_A, and then a few minutes to calculate the orbits.

Since we calculated the orbits on $\Omega_8[2] \oplus A$ explicitly, we knew the stabilizer sizes and thus could employ randomized techniques to calculate the stabilizer for each orbit representative C of $(\Omega_8[2] \oplus A)/G_A$.

Finally, the orbits of $G_{C \oplus A}$ on $\Omega_8[1] \oplus C \oplus A$, a set of cardinality 2^8, were calculated. The difficulty here lies in the number of choices $C \oplus A$ that needed to be considered. In the most extreme case, the stabilizer of A has cardinality 192 (compared to $|G| = 5348063769211699200$), and there are 1424416 choices for C, resulting in 359052160 code loops with associator A. This case took several hours to complete.

Remark 4.1. Currently, Hora and Pudlák seek to classify the trilinear alternating forms on $V = \mathbb{F}_2^9$. They report that among the trilinear alternating forms on V is one having trivial automorphism group. By Corollary 3.8, this form alone contributes $2^{\binom{9}{1}+\binom{9}{2}} = 2^{45}$ pairwise non-isomorphic code loops of order 2^{10}. By contrast, there are $49\,487\,365\,422 \leq 2^{36}$ groups of order 2^{10} [2]. We expect that there are also forms with very small automorphism groups; the associated orbit calculations required in Corollary 3.8 may be infeasible.

The detailed results for $16 \leq n = 2^{d+1} \leq 512$ are summarized in Table 2. In the first column we give the dimension d of the underlying vector space over $\mathbb{F}_2$ and the order $n = 2^{d+1}$ of the resulting code loops, in the second column we list the ID for a trilinear alternating form A on $\mathbb{F}_2^d$ (an eventual associator map), in the third column we list the trilinear alternating form A (our numbering and choice of basis follow those of [21]), in the fourth column we list composition factors, with multiplicities, of the stabilizer G_A of A in $GL(d, \mathbb{F}_2) = L_d(2)$ (using the standard notation of [8]), in the fifth column we give the order of G_A, in the sixth column we give the number of orbits of G_A on $\Omega_d[2] \oplus A$ (eventual commutator maps), and in the last column we give the number ℓ_A of code loops with associator A up to isomorphism.

If $d \leq 7$ or $|G_A| > 10000$, then we stored all orbit representatives of the action of $GL(d, \mathbb{F}_2)$ on Ω_d, from which the code loops can be explicitly constructed using the method of [25]. In the

d/n	ID	A	factors of G_A	$\lvert G_A\rvert$	C_A	ℓ_A
3/16	0	$\emptyset$	$L_3(2)$	168	2	5
	1	123	$L_3(2)$	168	2	5
4/32	0	$\emptyset$	$L_4(2)$	20160	3	7
	1	123	$L_2(7)$, 2^3	1344	4	16
5/64	0	$\emptyset$	$L_5(2)$	9999360	3	8
	1	123	$L_2(7)$, 2^7, 3	64512	7	33
	2	123+345	A_6, 2^5	11520	9	47
6/128	0	$\emptyset$	$L_6(2)$	20158709760	4	10
	1	123	$L_2(7)^2$, 2^9	14450688	10	52
	2	123+345	A_6, 2^{10}	368640	22	174
	3	123+456	$L_2(7)^2$, 2	56448	20	224
	4	123+345+156	$L_2(7)$, 2^8	43008	19	234
	5	123+234+345+246+156	$L_3(4)$, 2, 3	120960	10	73
7/256	0	$\emptyset$	$L_7(2)$	163849992929280	4	11
	1	123	$L_2(7)$, A_8, 2^{12}	13872660480	13	72
	2	123+345	A_6, 2^{16}, 3	70778880	40	381
	3	123+456	$L_2(7)^2$, 2^7	3612672	53	903
	4	123+345+156	$L_2(7)$, 2^{14}	2752512	57	968
	5	123+234+345+246+156	$L_3(4)$, 2^7, 3	7741440	23	269
	6	123+345+567	2^{13}, 3^2	73728	289	10019
	7	123+145+167+357	$L_2(7)$, 2^{12}	688128	69	1459
	8	123+167+246+357	2^{10}, 3^2	9216	634	39916
	9	123+145+167	$Sp_6(2)$, 2^6	92897280	23	167
	10	123+145+167+246+357	$U_3(3)$, 2	12096	324	25052
	11	123+234+345+246+156+367	A_5, 2^{11}, 3	368640	67	1609
8/512	0	$\emptyset$	$L_8(2)$	5348063769211699200	5	13
	1	123	$L_2(7)$, $L_5(2)$, 2^{15}	55046716784640	16	92
	2	123+345	$L_2(7)$, A_6, 2^{20}	63417876480	59	627
	3	123+456	$L_2(7)^2$, 2^{14}, 3	1387266048	104	2040
	4	123+345+156	$L_2(7)$, 2^{21}, 3	1056964608	110	2181
	5	123+234+345+246+156	$L_3(4)$, 2^{14}, 3^2	2972712960	46	603
	6	123+345+567	2^{20}, 3^2	9437184	910	42058
	7	123+145+167+357	$L_2(7)$, 2^{19}	88080384	213	6157
	8	123+167+246+357	2^{17}, 3^2	1179648	1968	162636
	9	123+145+167	$Sp_6(2)$, 2^{13}	11890851840	59	655
	10	123+145+167+246+357	$U_3(3)$, 2^8	1548288	978	100396
	11	123+234+345+246+156+367	A_5, 2^{18}, 3	47185920	201	6588
	12	123+345+678	$L_2(7)$, A_6, 2^5	1935360	942	76858
	13	123+145+178+246	2^{18}, 3^2	2359296	1175	72552
	14	123+145+268+347	2^{11}, 3^2	18432	25352	4553608
	15	123+345+567+178	2^{15}, 3^2	294912	3121	340812
	16	123+145+168+246+257	2^{17}, 3	393216	2718	269244
	17	123+145+168+347+256	2^{10}, 3	3072	108136	24014336
	18	123+145+168+347+267	2^{14}, 3	49152	9050	1597720
	19	123+145+278+356+467	2^8, 3^2	2304	129180	30780784
	20	123+145+178+246+258+347	2^{13}, 3	24576	14252	2962796
	21	123+145+168+347+258+267	2^6, 3	192	1424416	359052160
	22	123+145+257+278+368+467	$L_2(7)$, 2	336	808692	204763400
	23	123+145+168+246+257+356+456	A_5, 2^{13}, 3	1474560	718	65885
	24	123+145+257+258+268+348+467	$L_2(8)$, 2^6, 3	96768	3392	732448
	25	123+145+167+178+258+267+347+356	2^9, 3, 7	10752	25952	6424768
	26	123+145+178+246+258+347+356+456	2^4, 3^3	432	628452	159271112
	27	123+145+258+356+478+567	2^8, 3	768	381912	92169184
	28	123+145+167+246+257+267+368	2^{10}, 3	3072	99452	23205904
	29	123+145+246+468+578	2^{10}, 3	3072	109276	24331744
	30	123+145+258+347+368+567	A_5, 2^8, 3	46080	9132	1686096
	31	123+145+457+678	2^{10}, 3^4	82944	6982	1096100

TABLE 2. The number ℓ_A of code loops with associator map A

remaining situations, we only counted the number of representatives. More detailed data files are available on request from the second author.

4.3. **Specific code loops and their automorphism groups.** We conclude by commenting on specific code loops and their automorphisms.

Lemma 4.2. *Let Q be a Moufang loop and let Z be a cyclic central subloop of Q such that Q/Z is at most 2-generator. Then Q is a group.*

Proof. Let $Z = \langle z \rangle$ and $Q/Z = \langle xZ, yZ \rangle$. Then $Q = \langle x, y, z \rangle$ and $A(x, y, z) = 1$ because z is central. By Moufang's Theorem [24], Q is a group. □

Lemma 4.3. *Every nonassociative Moufang loop of order* 16 *is a code loop.*

Proof. Recall that every Moufang 2-loop Q is centrally nilpotent [17]. If $|Q| \leq 8$ then there is $Z \leq Z(Q)$ of order 2 such that $|Q/Z| \leq 4$, so Q/Z is at most 2-generator and Q is a group by Lemma 4.2.

Suppose now that $|Q| = 16$ and Q is not associative. Let $Z \leq Z(Q)$ have order 2. Then Q/Z is a group of order 8 by the first paragraph, and Q/Z is not generated by any two of its elements by Lemma 4.2. Hence Q/Z is the elementary abelian group of order 8. □

There are 5 nonassociative code loops of order 16 according to Table 2, and thus precisely 5 nonassociative Moufang loops of order 16 by Lemma 4.3. This agrees with the classification of [5]. The automorphism groups of these 5 loops are as follows: soluble groups of order $2^4\,3$, 2^6 and $2^6\,3$ (twice); and a group of order 1344 with composition factors $L_2(7)$, 2^3. The last loop is the *octonion loop* $\mathbb{O}_{16}$ that captures the multiplication rules among the eight basic octonionic units and their additive inverses.

There are 71 nonassociative Moufang loops of order 32; among them are 16 code loops. The unique such code loop with the largest automorphism group (and composition factors $L_2(7)$, 2^7) is the direct product of $\mathbb{O}_{16}$ with the cyclic group of order 2.

The most famous code loop, the *Parker loop* $\mathcal{P}$, is obtained as the code loop of the extended binary Golay code $\mathcal{G}_{24}$ of dimension 12 (and hence is not found in our classification). The automorphism group of $\mathcal{G}_{24}$ is the Mathieu group M_{24}, and the group of so-called *standard* automorphisms of $\mathcal{P}$ (those automorphisms that belong to M_{24} when signs of elements of $\mathcal{P}$ are ignored) has structure $2^{12} \cdot M_{24}$ [10, Chapter 29].

A potentially rewarding research program is to investigate nonassociative code loops with "large" or "interesting" automorphism groups.

Acknowledgment

Petr Vojtěchovský thanks the Department of Mathematics, University of Auckland, for its hospitality and for access to its high performance computing facility.

The GAP code used in the implementation of our algorithm, although completely rewritten and highly optimized for speed, originated from the code of [26].

We thank Gábor Nagy, the referee and editor for helpful comments and suggestions.

References

[1] Michael Aschbacher, *Sporadic groups*, Cambridge Tracts in Mathematics **104**, Cambridge University Press, 1994.

[2] Hans Ulrich Besche, Bettina Eick and E.A. O'Brien, *A millennium project: constructing small groups*, Internat. J. Algebra Comput., **12**, 623–644, 2002.

[3] W. Bosma, J. Cannon, and C. Playoust, *The* Magma *algebra system I: The user language*, J. Symbolic Comput. **24** (1997), 235–265.

[4] Richard Hubert Bruck, *A survey of binary systems*, Ergebnisse der Mathematik und ihrer Grenzgebiete. Neue Folge, Heft **20**, Springer Verlag, Berlin-Göttingen-Heidelberg, 1958.

[5] Orin Chein, *Moufang loops of small order*, Mem. Amer. Math. Soc. **13** (1978), no. **197**.
[6] Orin Chein and Edgar G. Goodaire, *Moufang loops with a unique nonidentity commutator (associator, square)*, J. Algebra **130** (1990), no. **2**, 369–384.
[7] Arjeh M. Cohen and Aloysius G. Helminck, *Trilinear alternating forms on a vector space of dimension* 7, Comm. Algebra **16** (1988), no. **1**, 1-25.
[8] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, and R.A. Wilson. *Atlas of finite groups*. Oxford University Press, 1985.
[9] J.H. Conway, *A simple construction for the Fischer-Griess monster group*, Invent. Math. **79** (1985), no. **3**, 513–540.
[10] J.H. Conway and N.J.A. Sloane, Sphere Packings, Lattices and Groups, second edition, A Series of Comprehensive Studies in Mathematics **290**, Springer, 1993.
[11] Aleš Drápal and Petr Vojtěchovský, *Moufang loops that share associator and three quarters of their multiplication tables*, Rocky Mountain J. Math. **36** (2006), no. **2**, 425–455.
[12] Aleš Drápal and Petr Vojtěchovský, *Code loops in both parities*, J. Algebraic Combin. **31** (2010), no. **4**, 585–611.
[13] The GAP Group, GAP – *Groups, Algorithms, and Programming, Version* 4.7.8; 2015, http://www.gap-system.org
[14] Bettina Eick and E.A. O'Brien, *Enumerating p-groups*, J. Austral. Math. Soc. **67** (1999), 191-205.
[15] Bettina Eick, E.A. O'Brien and C.R. Leedham-Green, *Constructing the automorphism group of a p-group*, Comm. Algebra, **30**, 2271-2295, 2002.
[16] George Glauberman, *On loops of odd order. II.*, J. Algebra **8** (1968), 393–414.
[17] G. Glauberman and C.R.B. Wright, *Nilpotence of finite Moufang* 2*-loops*, J. Algebra **8** (1968), 415–417.
[18] Edgar G. Goodaire, Sean May and Maitreyi Raman, *The Moufang loops of order less than* 64, Nova Science Publishers, Inc., Commack, NY, 1999.
[19] Robert L. Griess, Jr., *Code loops*, J. Algebra **100** (1986), no. **1**, 224–234.
[20] Robert L. Griess, Jr., *A Moufang loop, the exceptional Jordan algebra, and a cubic form in* 27 *variables*, J. Algebra **131** (1990), no. **1**, 281–293.
[21] Jan Hora and Petr Pudlák, *Classification of* 8*-dimensional trilinear alternating forms over* $GF(2)$, Comm. Algebra **43** (2015), no. **8**, 3459–3471.
[22] Tim Hsu, *Moufang loops of class* 2 *and cubic forms*, Math. Proc. Cambridge Philos. Soc. **128** (2000), no. **2**, 197–222.
[23] Tim Hsu, *Explicit constructions of code loops as centrally twisted products*, Math. Proc. Cambridge Philos. Soc. **128** (2000), no. **2**, 223–232.
[24] Ruth Moufang, *Zur Struktur von Alternativkörpern* (German), Math. Ann. **110** (1935), no. **1**, 416–430.
[25] Gábor P. Nagy, *Direct construction of code loops*, Discrete Math. **308** (2008), no. **23**, 5349–5357.
[26] Gábor P. Nagy and Petr Vojtěchovský, *The Moufang loops of order* 64 *and* 81, J. Symbolic Comput. **42** (2007), no. **9**, 871–883.
[27] Gábor P. Nagy and Petr Vojtěchovský, LOOPS, version 3.1.0, package for GAP, http://www.math.du.edu/loops
[28] Thomas M. Richardson, *Local subgroups of the Monster and odd code loops*, Trans. Amer. Math. Soc. **347** (1995), no. **5**, 1453–1531.
[29] Petr Vojtěchovský, *Combinatorial aspects of code loops*, Loops'99 (Prague), Comment. Math. Univ. Carolin. **41** (2000), no. **2**, 429–435.
[30] Harold N. Ward, *Combinatorial polarization*, Discrete Math. **26** (1979), no. **2**, 185–197.

(O'Brien) Department of Mathematics, University of Auckland, Private Bag 92019, Auckland, New Zealand

E-mail address: e.obrien@auckland.ac.nz

(Vojtěchovský) Department of Mathematics, University of Denver, 2280 S Vine St, Denver, Colorado 80112, U.S.A.

E-mail address: petr@math.du.edu